キーボードタイピングにおける手の骨格情報をもとにした認証手法の提案

山北　将平 *　小高　知宏 *　黒岩　丈介 **　白井　治彦 ***

Authentication Method by the Keybord Dynamics using the Hand Skelton Infomation

Shohei YAMAKITA*, Tomohiro ODAKA*, Jousuke KUROIWA and Haruhiro SHIRAI*****

(Received February 6, 2015)

In this paper,we implement authentication system based on the the biometric characteristics of hand motion.We propose the authentication method using the hand skeleton information to improve the accuracy of the authentication.There is a keystroke dynamics authentication in previous research.It is an authentication method using individual differences keystroke biometrics.We employ the camera to detect feature value of keystroke.This method reads the skelton from the camera image.We use NimbleSDK to track to the hand.It is a high-performance tracking middleware.It minimizes the risk of false recognition.We evaluate the correlation of a rank of skelton.To examine the similarity, we use the Spearman's rank correlation coefficient.We devise an authentication method based on this evaluation value.Further, incorporate it into the password authentication.According to the method, high level of safety can be ensured.

Key words : Authentication,Biometrics,Seculity,Hand Tracking,Correlativity

1. はじめに

近年ではシステムを利用する際, 正規ユーザであることを認証することがほぼ必須となっている. コンピュータへのログイン, 銀行の ATM での引き下ろし, 出欠管理など用途は様々である. 多くの場合これらの認証に用いるものはユーザ ID とパスワードである. これは非常に簡単な仕組みでできている. 認証に必要なユーザ ID とパスワードのふたつのみであり, これらのキーワードを一致させることができれば認証を通過することができる.[1][2]

パスワード認証を突破するための方法は数多くある. 中でも代表的なものとして総当り攻撃（ブルートフォースアタック）がある. これは暗号などで理論的に取りうるパターンのすべてを入力し解読する方法である. 取りうる文字の種類, 長さによって必要となる時間が大きく変動する. しかし, 時間的制約が存在しない場合は確実にパスワードを調べることができる. このことから, パスワード認証は認証としてのセキュリティ性に重大といえる欠陥を抱えていると言える.[3]

パスワード認証のセキュリティ対策として一般的にあげられるのは, パスワードを盗み出されないようにする方法である. そのため, パスワードを盗み出さ

*原子力・エネルギー安全工学専攻
**知能システム工学専攻
*** 工学部技術部
*Nuclear Power and Energy Safety Enginnering course, Graduate School of Enginnering.
**Human and Artifical Intelligent Systems Course, Fraduate School of Engineering
***Dept. of Techenical,Dept. Engineering

れてしまった後,第三者が悪用できないようにする対策はなされていない.悪質な手口による不正アクセスが増加する中,盗みだしたパスワードが第三者に利用可能なことは,一刻も早く対策すべき問題である.

正規ユーザ本人にしか認証を通過させない技術のひとつとしてバイオメトリクス認証がある.これは人間の身体的特徴や行動的特徴をもとに人物の認証を行う仕組みであり,本人しか持ち得ない特徴をもとに認証を行う.モデルデータやテンプレートと呼ばれるユーザ本人を示す指標と認証時のセンサ情報から算出した値を比較することで認証を行う.[4]

バイオメトリクス認証を実装するには,対象となるシステムに対し生体情報を読み取るための機器を取り付ける必要がある.そのための取り付ける機器に応じてコストがかかってくる.実装コストの影響は製品の価格などユーザに対して直接的に関わってくる問題であるため,可能な限りコストは削減できることが望ましい.[5]

このような問題に対し先行研究ではキーストロークタイピング認証が存在する.これは人のキーストロークが独自の特徴を取ることを利用した手法である.しかし,動作をもとにした認証であることから指紋認証のような人体の形状をもとにした認証と比べ精度が劣るとされている.[6]

そこで本研究では,近年コンピュータに取り付けられていることが多くなったカメラを利用し認証を行う方法を提案する.キーボードのタイピングが独自の特徴を取ることを利用した認証方法があるように,タイピングする手の形状を見ることで認証する方法を考案する.この認証をパスワード認証と組み合わせる形で実装することで,ユーザログイン認証時のセキュリティ性を向上させる.

手の形状をもとに評価値を算出する方法として,本研究では手の骨格情報に着目した.タイピングの仕方が異なれば,タイピングする際の指の位置取りや曲げ方などに個人差が生まれる.このことから,タイピング時の骨格点の並び方にはユーザ独自の特徴が現れるのではないかと推測される.この並び方の特徴性を調べるため,スピアマンの順位相関係数を用いる.[7] この手法はチャールズ・スピアマン (Charles Spearman) によって提唱された,統計学における順位データからの相関の指標である.これを用いることで,入力データとモデルデータとの間における,手の並び方の相関性を調べることで類似性を算出する.

本研究ではコンピュータを操作する手の動作をもとに人物の認証を行う手法を開発する.これにより,不正なユーザにパスワードの漏洩や盗難が起こってしまった場合でも,侵入を阻むことができセキュリティの向上を図ることができる.また既存の認証手法の問題となっているコスト面の解決,他人受入・本人拒否の危険性を取り払うことができるシステムの開発を行う.

2. コンピュータ利用における認証技術

2.1 関連技術

既存の技術では,認証を突破するのに最適な手段を行使されると侵入を許してしまう.パスワード認証の不正対策は,複雑なパスワードにすることで総当たり攻撃などで解析されづらくするという方法が一般的である.しかし,このような対策はあくまで第三者に侵入されづらくするものであり,システムに侵入されないようにする対策ではない.

すべての機器に対して有効な認証は数少なくなりつつある.パスワード認証のように汎用性の高い認証は不正ユーザからすれば,侵入方法が確立されてしまっている.そのため,近年では従来手法に代わる様々な認証手法が考案されている.中でも生態的特徴をもとにしたバイオメトリクス認証という手法が注目されている.これは人のもつ身体・動作の特徴をもとにした認証である.各個人が持つ独自の生態的特徴をもとにしているため,第三者に悪用される危険性が極めて少ない.しかし,バイオメトリクス認証は生態的特徴という特有のデータを収集するために,多くの場合は別途センサ機器を取り付ける必要がありコストがかかってしまう.

これに対し,予め機器に取り付けられているハードウエアを利用することでコストを抑えることが可能である.また,「コンピュータ利用においてのみ」といったように条件を限定することにより,その条件に特化した認証を実装できる.コンピュータ操作であればキーボードのタイピングリズム,スマートフォンであればタップ操作を利用した技術がある.これらの方法であれば,既存のハードウエアが利用可能であるためコストを抑えることができる.

以下に,このような方法で実装されているバイオメトリクス認証を説明する.

2.1.1 キーストローク認証

キーストローク認証はキーボードを使用する機器に用いられる認証手法である.一般的にはコンピュータを対象とした技術である.コンピュータは例外を除き周辺機器としてディスプレイやキーボードを使用

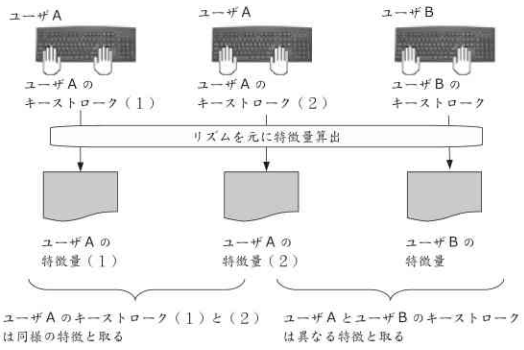

図 1: キーストローク認証における特徴性の差異

する. そのため, キーボードはコンピュータに付属されている機器ともいえる. バイオメトリクス認証には特徴性を読み取るために, 専用のセンサー機器が必要だと前述した. この認証手法ではキーボードという既存の機器を利用することでコストを抑えることが可能である.

認証方法には予めユーザのキーストローク収集し, モデルとなるデータを保管しておく必要がある. これを認証時の入力と比較することで正規ユーザであるかどうかを判別する. 入力データの収集方法は研究により様々である. 長期的に入力を監視し, 正規ユーザでないと判別した時点でシステムから弾くものもあれば, 短期的にパスワードのような定められたタイミングのみを監視し, 照合を行うものもある.

キーストローク認証の概要を図 1 に示す. キーストローク認証では入力内容の特徴で認証を行うことはしない. 特徴量として用いるものは一般的に打鍵のリズムである. 図 1 に示すユーザ A のキーストローク（1）と（2）はそれぞれ同様の特徴を取る. それに対して, ユーザ A とユーザ B では異なる特徴を取る. さらにユーザ C, ユーザ D と人数を増やしても同様で, キーストロークリズムは各人物ごとに独自の特徴をもっている. よって, それぞれのユーザごとにモデルを作成し, 認証時の入力に対して照合を行うことで, 正規のユーザであるかが判別可能である. パスワード認証にこの認証を組み合わせた手法の流れを以下に示す.

1. ユーザ登録時に数回のタイピングを行い, ユーザプロファイルとして保持する
2. 認証時に入力したユーザ ID とパスワードが一致するかをチェックする
3. 認証時に取得した時間ベクトルを特徴抽出ユニットに通して, 特徴ベクトルに変換する. この時の特徴ベクトルをテスト署名とする
4. ユーザプロファイルに保持された時間ベクトルを特徴抽出ユニットに通して, 特徴ベクトルにする. この時の特徴ベクトルからリファレンス署名を計算する
5. リファレンス署名とテスト署名を比べる事によって認証を行う
6. 認証に成功した揚合, 取得した時閥ベクトルをユーザプロファイルに加える

この研究ではリズムを意識した入力を行うことで, 精度が向上したという結果が得られている.[8] また短いパスワードでは許容可能な範囲まで改善されることはなかったと述べられている. リズムという特徴を検出するに十分な入力が, 短い入力では検出できない. 短期的な入力をもとに認証を行うには, それに特化したルールの作成が課題である.

2.1.2 フリック認証とタッチジェスチャー認証

フリック認証とタッチジェスチャー認証は近年普及しているスマートフォンなどの分野で用いられる認証手法である. スマートフォンとはタッチパネルで操作を行う携帯端末のことである. 画面上を指で払うように動かすことで, ページのスクロールや項目の移動を行う. このような動作を「フリック」と呼ぶ. また, 文字入力にはボタン式の入力方法とは異なり, この方法を利用したフリック入力と呼ばれる方式が採用されている.

同様に, タッチジェスチャーもスマートフォンなどを操作するのに使用される方法である. スマートフォンはマルチタッチに対応した設計がなされている. 複数の指である決められたジェスチャーをすることで特別な操作が可能となる. 画面上に 2 本の指を置き間隔を狭めることでピンチイン, 間隔を広げることでピンチアウト, といった操作ができる. これらのジェスチャーを使用することで, 画面の縮小・拡大を直感的に行うことができる.

これらの操作をもとに, スマートフォン独自の認証を考案したものがフリック認証とタッチジェスチャー認証である. 先行研究では, ニューラルネットワークモデルの一つである自己組織化マップ（SOM : Self-Orgnizing Maps）をもとに, 競合信号を基礎とした教師なし学習を行う.[9]SOM はクラスタリング手法と

比べ正確性に優れている. また, 多次もとデータでのユークリッド距離よりも認証精度が高い. この研究では, 認証精度 90.87 %から 98.01 %という結果が得られている. 精度の幅は着席・直立姿勢, 端末を保持する手の利き手・逆手によるものであり, 精着席姿勢で利き手で端末を保持している場合が最も精度が高いという評価がなされている. この手法はスマートフォンのロックを解除した後の画面で動作するよう実装することを用途としている. ユーザの操作を継続的に監視することや, 画面のレイアウトにあわせた評価方法の考案が課題となっている.

2.1.3 ハンドジェスチャー認証

ハンドジェスチャー認証とは, 手で指定の動作を行うことで認証を行う方法である. カメラや赤外線センサーを用いて, 手のジェスチャー情報を収集する. 先行研究では, 空中に署名を行う動作情報をもとにした認証手法がある.[10]Kinect を使用し手の三次元情報を収集する. 座標点は「手」と認識された一点の座標のみを使用する. 署名する動作からのみ特徴抽出を行うため, 手の関節など細かな骨格の検出は行わない. 収集した手の位置座標の時系列データを正規化し, モデルとの類似度を DP マッチングを用いて計算する. この結果が判定基準を満たしている場合は本人である可能性が高いと判断する.

この研究ではデータ計測方法の確立が急務であるとされている. 手の位置座標時系列を取得する際の位置ずれや, 手・肘などの座標が重なり誤認識を生むことが問題としてあげられる. カメラ情報を用いた認証には正確なデータ計測が重要な課題であるといえる.

2.2 従来の手法の問題点とその解決方法

本研究では, キータイピングをする人物の手の骨格情報をもとにしたバイオメトリクス認証を考案する. このシステムを構成するにあたり, 解決すべき従来の手法の問題点を以下にまとめる.

はじめに, 短い入力での認証精度に対する問題である. キーストロークダイナミクス認証のような手法では, 収集するデータ量が多ければ多いほど高い精度が期待できる. その反面, 認証に用いる入力データが少ない場合の精度は低くなりがちである. これに対して, 時間あたりに収集するデータ量を増やすことによってこの問題を解決する. 1 イメージあたりに収集する手の骨格情報を出来る限り細分化する. 指先や手の付け根だけでなく, 各指の関節座標の収集も行う.

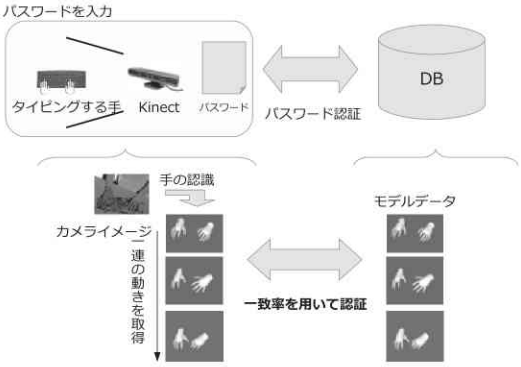

図 2: 本認証システムの構成図

これにより短時間の入力データでも, 高精度の結果を得るに十分な情報量を期待できる.

次に, ユーザが行う動作にばらつきが出てしまう問題である. スマートフォンにおける認証では, 普段の姿勢や操作する手が異なると, 操作時の動作が安定せず認証精度が低下することがわかっている. 本手法はキーボードタイピングを行う手の動きをもとに認証をする. そのため, 座った姿勢でキーボードをカメラの中心になるよう環境を定める. また, 本手法をパスワード認証と組み合わせることで実装する. 入力内容をパスワードのように短い入力内容にすることにより, 独自のリズムでのタイピングを再現することが容易になると考えられる.

最後に誤認識に関する問題である. ハンドジェスチャー認証のようにカメラ情報をもとにした認証では, 実際とは異なる体や物の座標を手だと誤認識してしまうことが問題となっている. このことから, 認証システムとして十分なトラッキング性能を実現する必要がある. しかし, 人体の形状を正確に認識することは極めて難しい. これにはトラッキング用のミドルウェアを利用することで解決する. その中でも, 手の形状認識に優れた SDK を利用することで誤認識の危険性を最小限に抑えることができる.

2.3 本認証システムの構成

本研究で実装する認証システムの構成について説明する. 従来の手法の問題点で述べた項目を解決することで, 既存の手法よりもセキュアな認証システムを構築する. 本研究で構成をするシステムを図 2 に示す.

システムが認証に至るまでの流れについて説明する. まず, システムからユーザに対しパスワードの入

力を求める. これに対しユーザはカメラである Kinect に手が映る状態でパスワードを入力する. そして, この入力内容であるパスワードをデータベース上に保存された正解のパスワードと照合する. これは一般的に使用されているパスワード認証と同様のものである. これと並行し, パスワード入力を行う手を写したカメライメージを読み込む. このイメージをもとに手の認識を行い, パスワードを入力する一連の動作を取得する. この入力データをデータベース上に保存されているモデルデータと照合する. その照合には一致率を使用する. バイオメトリクス認証のように, 入力がモデルデータと完全に一致することのないような認証方法の場合, 一致の度合いを測る必要がある. この一致率が定められた閾値を上回れば認証を許可する.

このシステム構成を行うに際し説明した流れは, 大きく分けて 3 段階に分類される.

（1）データ収集

（2）特徴量抽出

（3）照合

それぞれを構成するのに必要となる事項について説明する.

（1）データ収集

まず, ユーザの認証に必要なデータを収集する. 本研究では認証に使用するデータに, パスワードを入力する手の動作を使用する. そのため, まずは手の動作をもとにした認証を行う前に, 通常のパスワード認証を行う. このために, 事前にユーザのパスワードをデータベース上に保管しておく. また, パスワード入力時のキーイベントを調べることで, テキストフォームを利用したパスワード認証と同等の機能を有することができる.

手の動作に関しては,Kinect と NibmleSDK を使用することで骨格検出を行う.[11] 手の形状を調べるのに際し, 障害物による誤認識が起こりうることを考えられた. そこで NimbleSDK というトラッキング用のミドルウェアを使用することで, この危険性を回避した. 読み取った骨格データは三次元座標によって表される. これを使用し, 特徴量の抽出を行う.

（2）特徴量抽出

データ収集を行った後, 動作データをもとに特徴量の抽出を行う. これには予めユーザのモデルとなるデータを準備する必要がある. モデルデータは認証時同様にパスワードの入力を行い, 動作データを収集することによって生成する. このモデルデータと認証時の入力データのふたつを比較し一致率を求めることで, それを特徴量をする. データの比較方法には骨格の並びかたをもとに相関性を調べることで行う. この相関性を数値化するために, 本研究では Spearman の順位相関係数をもとに算出する.

（3）照合

以上の結果をもとに正規のユーザであるかどうかを照合する. これにはパスワード認証と動作認証のふたつを使用する. パスワード認証はデータベース上に保存されているもとの完全に一致していた場合のみ認証を通過する. それに対して動作認証では, 算出した一致率が閾値を上回っていた場合のみ認証を通過する. これは生体認証においてモデルデータが入力と完全に一致することはほぼありえないからである. この閾値の設定には実験を行い, それをもとに最適な数値を決定する.

本研究では以上のようなシステム構成をことで従来以上にセキュアな認証方法を提案する. 最終的な認証精度の算出には FRR（False Rejection Rate）/FAR（False Acceptance Rate）を使用して評価する. これは本人拒否率/他人受入率と呼ばれるものであり, 誤認証の比率を表す.FRR は正規ユーザであるにもかかわらず他人であると認証を拒否してしまうことであり,FAR は他人であるにもかかわらず正規ユーザであると認証を許可してしまうことである. このふたつの０％に近いほど正確な認証ができていると言える.

しかし, いずれの評価値も０％となる認証を構築することは極めて困難である. 製品化されたバイオメトリクス認証では一般的に FRR １％,FAR １％以上の精度をもっている. これをもとに, 本研究では, 目標とする認証精度を FRR １％,FAR １％とした.

3. 本認証手法の実装

本研究の認証を行うために用いる一致率の算出方法について述べる. ここでの一致率とは, 認証対象であるモデルに対して現在認証を行っているユーザがどれだけ類似しているか, ということを意味している. 本研究の認証には, 3 つのステップがある.

（1）キーごとの一致率

（2）パスワードの一致率

（3）閾値との比較

上記の手順を行うことで, 最終的な認証の許可・拒否を行う.

まず本研究で行う一致率の算出方法について説明する. 手法にはスピアマンの順位相関係数を使用する. この式を以下に示す.

$$\rho = 1 - \frac{6\sum D^2}{N^3 - N} \tag{1}$$

D は対応する値の順位差であり,N は値のペアの数である. 対応する値とは同一の骨格名を持つ座標点のことを表している. これを用いることで骨格の並び方の相関性について求めることができる. 値の取りうる範囲を以下に示す.

$$-1.0 <= \rho <= 1.0 \tag{2}$$

1.0 に近づくほど相関性は強く,-1.0 に近づくほど逆相関性が強い. また,0 に近づくほど相関性が弱いことを表している.

次に本研究の一致率算出に使用するデータについて説明する. 使用するデータはキー入力のタイミングに応じたものを利用する. そのタイミングを図 3 に示す. 縦軸はキーの入力がある場合は「ON」ない場合は「OFF」をとる. 横軸は時間軸を表している. 山なりになっている間はいずれかのキー入力が行われている. この図中の山なりになった瞬間のタイミング, つまり KeyPress イベントが発生した瞬間の手の形状を使用する. 図 3 では n 回のキー入力が行われているため, 1 パスワードあたり n 個のデータを使用して一致率を算出する.

次に, キーごとの一致率について説明する. 本手法では手の形状を 3 次元座標として認識する. その座標群のｘ, ｙ, ｚ座標それぞれを上記の手法である Spearman の順位相関係数によって相関係数を求める. その後, 三方向の値を平均することでキーごとの一致率とする.

次にパスワードの一致率を求める方法について説明する. パスワードの一致率はキーごとの一致率をもとにして算出する. そして求められたキーごとの一致率を総和し, キー数で割る. この一致率の平均をパスワードの一致率とし, (３) の閾値との比較に用いる.

最後に閾値をもとに許可・拒否の振り分けを行う. 最終的な結果は以下の二通りが考えられる.

全体の一致率 >= 閾値

このような条件となった場合, 閾値を上回る一致率であることから正規ユーザである可能性が極めて高い. そのため, 認証を通過させる.

全体一致率 < 閾値

対して閾値を下回った場合, 正規ユーザでない危険性が高い. よって, 認証を弾くことによって侵入を防ぐ. 以上が本手法の認証方法である.

4. 実験

本章では開発した手法の認証精度の検証を行う. 認証精度には FRR/FAR のふたつから調査する. 本稿で提案した手法が特徴性を表しているかを各パラメータごとに評価する実験, システムの認証精度を評価する実験のふたつを行う.

4.1 実験環境と実験用データの収集方法

今回の実験では, 本研究室の学生６名を対象にデータの収集を行った. パスワードは各自に１種類ずつ作成してもらい, 入力回数は各パスワードごとに１０回ずつ収集した.

実験ではモデルデータと入力データとの一致率をもとに評価を行う. 収集したデータをどのようにモデルデータ, 入力データと振り分けるかを図 4 に示す. この図中にあるモデルデータ名, 入力データ名は「(入力者):(パスワードの種類):(ｎ番目の入力)」の形で記述した. 「ユーザ A : パスワード A : 入力１」であれば, 「ユーザ A が, ユーザ A が作成したパスワードを, 第１回目に入力した」入力内容を使用しているということとなる. モデルデータとするのは入力者が作成したパスワードである. そのためモデルデータにはユーザ６名×入力１０の６０パターンを使用する .

本研究は漏洩したパスワードを悪用し, 第三者が不正にログインしようとする場面を想定する. そのため, モデルデータに対し入力データは同一のパスワードを入力している必要がある. パスワードの種類は被験者数分あるが, 実験で一致率算出に用いる組み合わせはモデルデータと入力データのパスワードが同一のものでのみ行う.

モデルデータと入力データの入力者が同じであった場合について述べる. これは正規ユーザが正規の方法でシステムにログインしようとしていることを意味する. この場面において認証を拒否した場合は本人拒否が起きている. 正規ユーザのログインが失敗したことから, 本人拒否が起きていることが結果として得られる.

次にモデルデータと入力データの入力者が異なる場合について述べる. これは第三者が不正な方法で入手したパスワードを用いてシステムにログインしようとしていることを意味する. この場面において認証を許可した場合は他人受入が起きている. 不正な方法

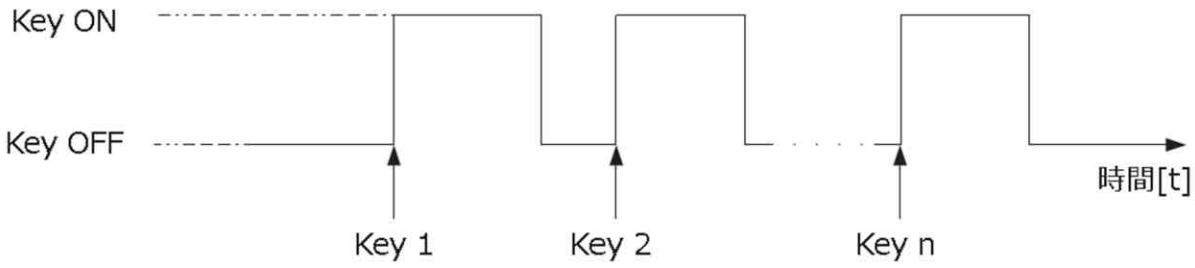

図 3: 利用するキー入力のタイミング

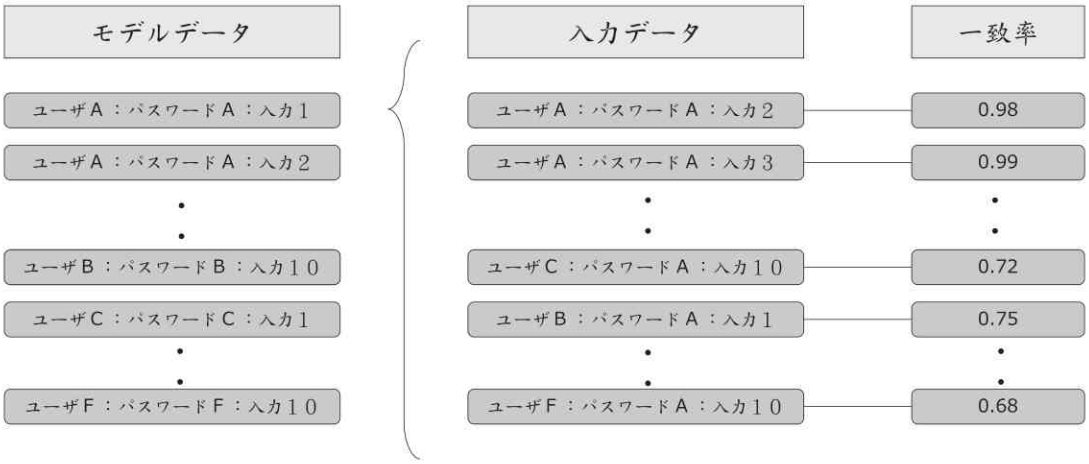

図 4: 比較するデータ

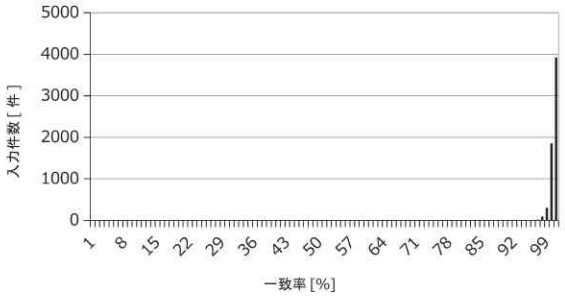

図 5: ｘ軸における本人の一致率分布

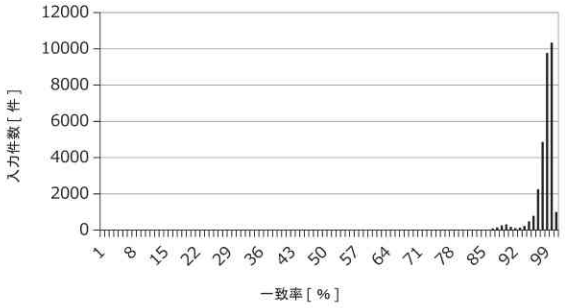

図 6: ｘ軸における他人の一致率分布

でのログインを許してしまっていることから, 結果には他人受入が起きていることが結果として得られる.

4.2 パラメータごとの特徴性評価実験

入力された座標軸のパタメータごとに, 他人・本人がそれぞれ適した特徴性を表しているか調査する. 収集したデータをもとにｘ, ｙ, ｚ軸座標の三種類の一致率を算出する. 各一致率をグラフ化し, 本人・他人のそれぞれの一致率が異なる特徴をとっているかを調べる.

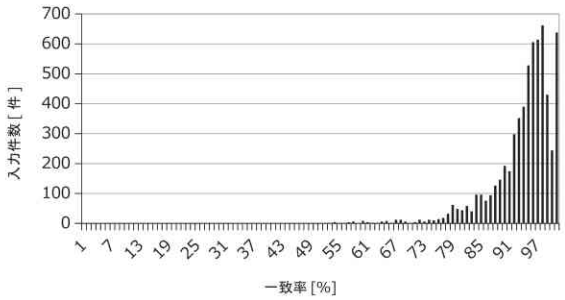

図 7: ｙ軸における本人の一致率分布

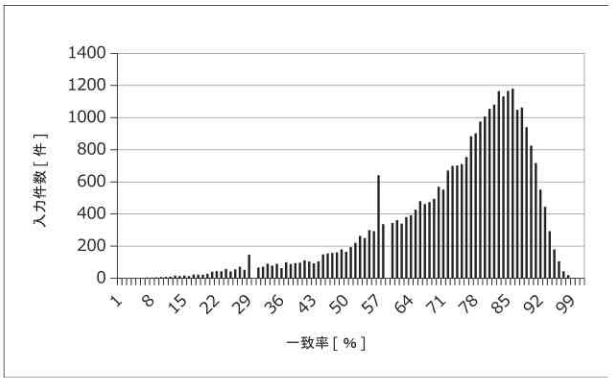

図 8: ｙ軸における他人の一致率分布

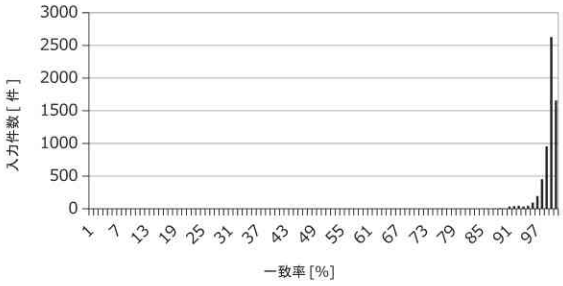

図 9: ｚ軸における本人の一致率分布

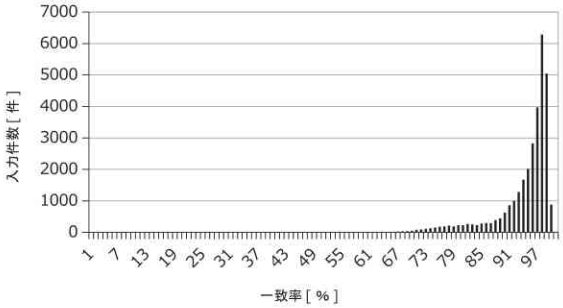

図 10: ｚ軸における他人の一致率分布

まず正規ユーザである本人の入力をもとにした一致率を図 5 図 7, 及び図 9 に示す. 次に他人の入力をもとにした一致率を図 6 図 8, 及び図 10 に示す. これらの結果から, 本人によるものと他人によるものでは, 一致率に明確な差があることを立証できた. また, 座標軸ごとに取りうる値の域が異なっており, 本人の入力はより高い一致率付近に分布していることが確認された.

4.3 認証精度の評価実験

認証精度を本人拒否率, 他人受入率のふたつから調べる. 認証精度の調査結果を図 11 に示す. 縦軸が他人受入率, 横軸が本人拒否率を表しており, 閾値を変化させることでどのような値を示すかを表している. 本人拒否率, 他人受入率のふたつは相反関係にある. このことから, 閾値の設定によって FRR/FAR は大きく変動する. この 2 つの評価値が最小となるような閾値を設定することが望ましい. このように閾値を設定したところ, この実験から得られた結果では FRR4.4 %,FAR3.3 %となった.

次にユーザごとの結果を示す.FAR,FRR のふたつから認証精度の高かったユーザ, 低かったユーザのふたつに分けた. 認証精度の高かったユーザを図 12, 低かったユーザを図 13 に示す. それぞれの縦軸は他人受入率, 横軸は本人拒否率を表している.

まず図 12 の認証精度が高かったユーザについて述べる. これらのユーザにおいては高水準の結果が得られた. 特にユーザ C は FRR0.0 %,FAR0.0 %. であり最も理想的な結果であった.

次に低い精度のものについて示す. これらは実験結果 1 と比べ精度の低さが顕著である. また, 実験結果 1， 2 の 2 つの間に属するような結果が得られたユーザはおらず, このことからモデル生成の段階で何らかの問題が発生していることが考えられる.

5. 考察

本稿ではふたつの実験から, パラメータごとの評価と本手法そのものの評価を行った. それぞれから得られた結果を考察する.

パラメータごとの実験では収集した入力データをもとに, 各座標軸ごとに一致率を算出した. それぞれが本人の場合, 他人の場合で異なる値を示しているかを調査した. これにより, 本手法が正確な特徴性を取りうる手法として成立しているかどうかを調べた. 実験結果からは本人, 他人それぞれが明確に異なる一致率の取り方をしていたことが確認できた. 本人であれば一致率が高い域に多く分布しており, 他人であれば一致率が低い域に分布している.

最も本人と他人の一致率に差が生じたのはｙ軸による結果であった. ｙ軸における他人の一致率は他の軸の結果と比べ, 低い一致率の域に多く分布している. 不正なユーザの入力に対しては, 認証を弾くためにもできるかぎり低い一致率であることが望ましい. このことから, ｙ軸から得られた結果は各軸の中で最も理想に近いものであった. 本研究ではｘ， ｙ, ｚそれぞれを等しい重みで取り扱っているが, 今回の結果から重み付けによる評価が期待できると考えられる.

またｘ軸は最も差が小さいという結果となった. 他人の一致率の下限が７６％と他のパラメータと比べ明らかに高い値をとっている. しかし, 本人の一致率から見てみるとｘ軸は他と比べ高い特徴性を示していることが見受けられる. このことからｘ軸の結果をもとに, 低い一致率の入力に対する足切りが有効であると考えられる.

上記ふたつの結果が得られた理由について考察する. まず, ｙ軸における一致率で他人の入力が非常に低い値を多くとった理由として, 指の曲げ伸ばしができる方向がｙ軸に集中しているからだと考えられる. またｘ軸は左右の手の位置取りに左右される点が少ないことや, 指の曲げ具合によっても差が生まれずらいことから大きな差が見られなかったと考えられる.

次に認証精度評価実験について考察する. この実験では収集したデータをもとに本認証手の他人受入率, 本人拒否率を調査した. この実験をすることにより本手法の認証精度を確認できる. 図 11 に示された実験結果から, 本手法の精度は FRR4.4 %,FAR3.3 %であることがわかった.

まず認証精度が一見して高かったものを図 12 に示した. この結果では比較的理想に近い結果を取っている. これらのユーザは理想的な認証精度を示した. これらのユーザで平均をとると認証率は FRR1.0 %,FAR0.5 %であり, これは研究目標を上回る精度である.

これに対し図 13 に示すユーザに関しては非常に低い認証精度を示した. これらのユーザは前述したユーザと比べ明らかに異なる結果を表しており, モデル生成や手のトラッキングの段階で何らかの問題が生じている可能性が推察される. 今後はこの問題を解決することで, いかなるユーザも高い認証制度のユーザグループに属することができるようにすることが課題となる.

上述の課題を解決するため, 今後の展望を以下に述

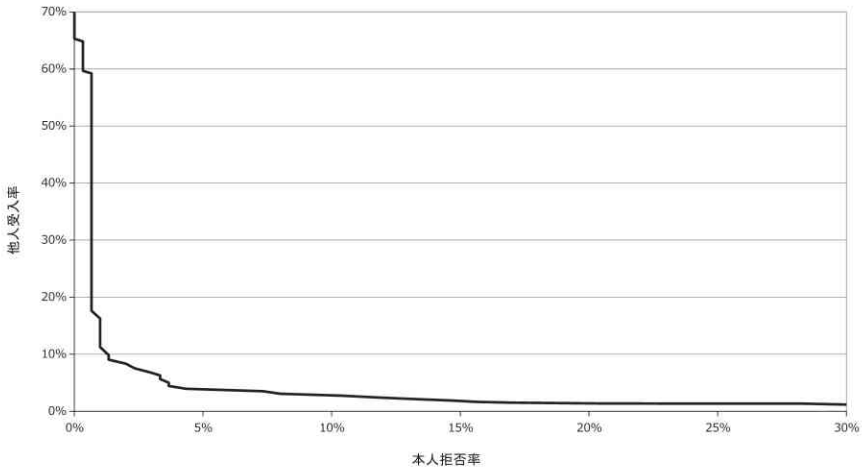

図 11: 認証精度

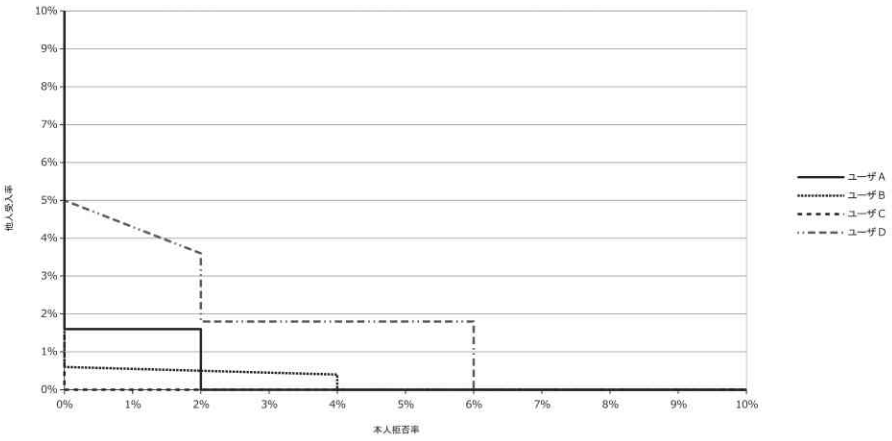

図 12: 実験結果 1

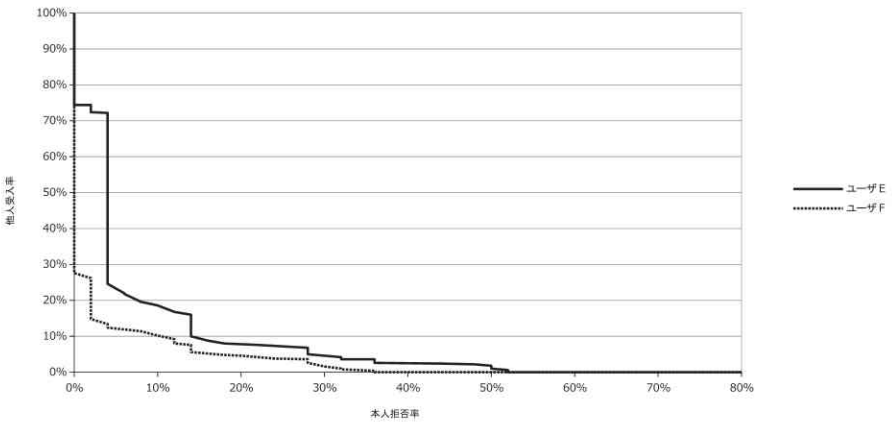

図 13: 実験結果 2

べる. 現在は手の誤認識を判別する機能の実装には至っていない. そのため, 精度が低かったユーザに誤認識が起きていた可能性も存在する. 手の形状データとして適した入力であったかを判別する必要がある. また, パスワードの文字列がユーザの特徴性を示すに適していなかった可能性も存在する. そのため, ユーザの特徴性を示しやすいパスワードの生成方法の考案やモデルの生成の段階で一定の特徴性を示しているかを確認する必要があると考えられる.

本研究で実装したシステムは従来の手法と比べ, 短いキータイピングでの認証に対応することができた. これには両手で４４点からなる骨格情報を利用したことがあげられる. 本来パスワードという短時間の入力では十分な特徴性を検出できない. それを補うに十分な情報量をカメライメージから収集することができたことが, 本研究結果に結びついていると考えられる. しかし, 本研究は短い入力に特化した手法であることから, 長いパスワードや複雑なパスワードは考慮していない. 従来の手法では長期的な入力であるほど, 精度は上がる傾向にある. それに対し, 本研究では長期的な入力であると, 入力の再現性が低くなり精度が低下してしまうと考えられる. 長期的な入力を使用して認証を行うためには, 新たに専用の手法を考案する必要がある.

実験では, 座った姿勢でのデータを収集した. また, キーボードはカメラの中心になるよう配置した. 認証に用いる入力内容も被験者に自分が打ちやすいパスワードを作成してもらうことで, タイピングの再現性を高くすることができたと考えられる. しかし, この方法ではシステムの設置場所を移行する際に, それまで収集したデータでは正確に認証が行えない可能性がある. キーボードを支点にカメラデータの位置合わせを行う機能の実装が必要と考えられる.

従来の研究ではトラッキングをする際, 肘や周辺にある物などを間違って手だと検出する誤認識が問題となっている. これに対し, 本研究では NimbleSDK というトラッキングのミドルウェアを利用した. 生体認証において, 特徴に用いる身体の部位を正確に検出することは極めて重要である. 高い精度で手のトラッキングを可能とする NimbleSDK を使用することで, 誤認識の危険性を最小限に抑えることができたと考えられる. しかし, 誤認識が起きていないかを確認するためにも, 手の形状が正確であるかを判別する機能の実装が必要と考えられる. この機能をデータ収集を行う部位に組み込むことにより, 収集したデータが正常であるかの判別が可能となる. 誤認識の可能性が高いと判断された入力は破棄し, 再入力を求めることでも, 他人受入や本人拒否の危険性を抑えられると考えられる.

6. まとめ

本稿ではコンピュータ利用における不正利用に対して, よりセキュリティ性の高い認証手法の考案を行った. コンピュータ利用における認証は一般的にユーザ ID・パスワードを用いた認証方法であるが, このような方法は総当りなど極めて簡単な方法での解析が可能でありその危険性については古くから問題視されてきた. そこで本研究では手の動作をもとに認証する仕組みをパスワード認証と組み合わせる形で実装した.

従来の研究から人の取る動作は各々全く異なる特徴性ととることがわかっている. コンピュータ利用における特徴性を検出するため, キーボードタイピングを行う際の手の動きに着目した. 入力するキーの内容に応じ人は事前に次の入力へと指を進ませる. そのため予備動作の違いから人により同じキーを入力する場合でも手の形状に特徴が生まれる. これを利用することで同じパスワード内容の入力を受けたとしても, 他人では特徴の違いから認証を通過することができない. これによりセキュアなシステム設計が可能となる.

本認証手法を実装するにあたり, ハードウェアにはキー入力を得るためにキーボード, 手の動きを検出するためにカメラとして Kinect を使用した. 手の動きを取得するため NimbleSDK というミドルウエアを利用した. これは手の骨格情報をトラッキングすることができるというものである.

実験結果から手の骨格情報が各自の特徴性を示していることが確認された. 特にｙ軸における順位相関係性が極めて高い. これは左右の手の位置取りにおいて, 並びに特徴が生まれやすいためであると考えられる. また, 実験から本手法の精度は FRR4.4 %,FAR3.3 %であるという結果が得られた. この結果をユーザごとに分け比較したところ, 精度が極めて高かったユーザと, 極めて低かったユーザという２つのグループが存在することがわかった. この２グループは差が極めて大きいことから, 精度が低いユーザグループには何らかの問題が生じている可能性が存在する. 今後はこの問題を解決することが研究の発展に繋がると考えられる.

問題を解決するためには以下のような方法が考えられる. まず第一に本手法の精度の水準そのものを引き上げることである. 実験からパラメータごとに

特徴が現れやすい座標軸が存在することが明らかとなった. 今回得られた結果をもとに重み付けを行うことで, 本手法全体の精度向上が図ることができると考えられる. 第二に手のトラッキングを行う機能の改善である. トラッキングの段階, 特にモデルの生成において骨格の誤検知により不正確な形状を記録してしまっている可能性が存在する. そのため, 手の形状や動きが正常であるかどうかを判別する機能が必要である. 第三にパスワードとユーザの相性関係があげられる. これには作成したパスワードがユーザに適合するものであるかを判別する機能, もしくはユーザの特徴性を引き出すのに最適なパスワードを生成する機能があげられる.

以上から, 本研究では手の骨格情報をもとに生体認証を行う手法を考案した. 実験結果から, 手の骨格情報をもとにした手法の有用性が検証することができた. 今後はパラメータごとに重み付けを行うことや, トラッキング機能の改良などを行うことによって, より高い水準の認証手法を確立することが可能であると考えられる.

参考文献

[1] 山北 将平, 小高 知宏, 黒岩 丈介, 白井治彦:手の動的特徴とキーストロークの組み合わせによる認証手法の提案, 電気関係学会北陸支部連合大会 (2013).

[2] 山北 将平, 小高 知宏, 黒岩 丈介, 白井治彦:手の動的特徴に基づく認証手法の提案, 電気関係学会北陸支部連合大会 (2014).

[3] 桑門 秀典, 森井 昌克:総当たり攻撃に対して安全な認証関数の構成法, 電気関係学会北陸支部連合大会,50-9,1930-1941 (2014).

[4] 鷲見 和彦:バイオメトリクスセキュリティ概論, 電子情報通信学会誌,89-1,27-30 (2006).

[5] 山元 規靖, 若原 俊彦:携帯電話搭載デジタルカメラと 2 次元カラーコードを用いたユーザ認証システムに関する考察, 電子情報通信学会技術研究報告,110-375,51-56 (2011).

[6] 村松 大吾:オンライン署名の可能性, ２００６年電子情報通信学会通信ソサイエティ大会 (2006).

[7] 笛田 薫:Spearman's rank correlation type two-sample test, 九州大学理学部紀要,47-1,27-39 (1993).

[8] 山村 直也, 鈴木 隼人, ラシキア 城治:打鍵署名を利用したパスワード認証の強化について, 情報処理学会研究報告,2009-20,79-84 (2009).

[9] 山田 健一朗, 納富 一宏, 斎藤 恵一:スマートフォン操作時における行動的特徴量を利用した個人識別手法, バイオメディカル・ファジィ・システム学会,16-1,41-48 (2014).

[10] 真部 雄介, 松尾 翔太, 菅原研次:空中での手の動きによる個人認証手法, 人工知能学会全国大会（第 26 回） (2012).

[11] 3Gear systems:Writing your own applications,http://nimblevr.com/latest/doc/api.html.